

TED STEVENS, ALASKA  
GEORGE V. VOINOVICH, OHIO  
NORM COLEMAN, MINNESOTA  
TOM COBURN, OKLAHOMA  
LINCOLN CHAFEE, RHODE ISLAND  
ROBERT F. BENNETT, UTAH  
PETE DOMENICI, NEW MEXICO  
JOHN WARNER, VIRGINIA

JOSEPH I. LIEBERMAN, CONNECTICUT  
CARL LEVIN, MICHIGAN  
DANIEL K. AKAKA, HAWAII  
THOMAS R. CARPER, DELAWARE  
MARK DAYTON, MINNESOTA  
FRANK LAUTENBERG, NEW JERSEY  
MARK PRYOR, ARKANSAS

MICHAEL D. BOPP, STAFF DIRECTOR AND CHIEF COUNSEL  
JOYCE A. RECHTSCHAFFEN, MINORITY STAFF DIRECTOR AND COUNSEL

**COPY**

## United States Senate

COMMITTEE ON  
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS  
WASHINGTON, DC 20510-6250

June 30, 2005

David M. Walker, Comptroller General  
Government Accountability Office  
441 G St., NW  
Washington, DC 20548

Dear Comptroller General Walker:

In 2003, the President's *National Strategy to Secure Cyberspace* recognized that America needed to be prepared for the possibility of debilitating cyber incidents and develop a national cyber disaster recovery plan. In 2003, the Congress amended the Defense Production Act (DPA) to clarify that the federal government could use these authorities to prioritize the delivery of products and services to speed recovery of critical infrastructures.

The federal government has long maintained detailed policies, plans, and programs to ensure voice communications in all circumstances. However, it is unclear what policies and programs the Department of Homeland Security (DHS) has developed as part of their national cyberspace security response to ensure that the nation has the requisite capabilities to recover key internet capabilities.

In addition, since the late 1990's the federal government has been developing capabilities for cyber analysis to provide comprehensive information on changes in threat conditions and newly identified system vulnerabilities, as well as timely warnings of potential and actual attacks. The primary challenges have included obtaining, analyzing, and synthesizing intelligence, law enforcement, technical data, and other information to identify patterns that may signal that an attack is underway or imminent. These challenges have impeded capabilities to conduct tactical analysis pertaining to individual cybersecurity incidents, and strategic analysis to determine the potential broader implications of individual incidents.

In 2002, DHS was assigned important responsibilities in cyberspace security. Subsequently, the President's *National Strategy to Secure Cyberspace* also stressed the need to improve cyber analysis functions. In 2003, *Homeland Security Presidential Directive 7* assigned the department the responsibility for establishing an indications and warning framework for cyberspace. This month, the President released a National Counterintelligence Strategy that highlighted the need to detect foreign intelligence penetrations of America's cyber systems. Clearly, developing cyber analysis capabilities are essential for protecting America from Current and future threats. We would like the Government Accountability Office (GAO) to pursue the following:

1. Evaluate DHS plans, programs and capabilities for recovering and reconstituting essential internet mechanisms in response to a debilitating disruption;
2. Identify any joint-industry documents that have been developed for recovering internet functions or other identified requirements;
3. Assess the extent to which the provisions of the Homeland Security Act and other laws such as the DPA might be used to support the development of collaborative Internet recovery plans with industry;

Moreover, GAO previously identified significant challenges related to cyberspace security, including the need for a strategic analytical capability for computer-based threats and a comprehensive government wide data-collection and analysis framework. Accordingly, we would like GAO to conduct a detailed review of federal capabilities for cyber analysis and identify pertinent functions or capabilities in the private sector that might assist federal efforts. Specifically, we would like GAO to pursue the following:

1. Identify the federal homeland security, law enforcement, defense, and intelligence organizations involved in analyzing and warning of computer-based attacks, and their roles, responsibilities, and processes;
2. Assess the gaps between necessary analysis and warning capabilities and the government's current capabilities;
3. Determine the cyber analysis and warning capabilities of non-federal entities;
4. Identify any impediments to developing federal capabilities, including technology, policy, law, or human capital;
5. Determine what tools and techniques are available to help agencies attribute cyber-based attacks and capture and maintain forensic evidence useful for law enforcement investigations and homeland security analysis.

Sincerely,



Tom Coburn, MD  
Chairman  
Subcommittee on Federal Financial  
Management, Government Information,  
and International Security



Tom Carper  
Ranking Member  
Subcommittee on Federal Financial  
Management, Government Information,  
and International Security



Joseph Lieberman  
Ranking Member  
Homeland Security & Governmental  
Affairs Committee